Liana Davis
02/11/24

Article Review 1 - Navigating the Intersection of AI and Cybercrime: A Societal Perspective

In the realm of technology and cyber ethics, "Understanding the Application of Artificial Intelligence in Cybercrime" is an exploration of AI's role in transforming criminal behavior. The purpose of this review is to analyze the article's discussion of AI's dual nature, which can also be viewed as a tool for enhancing cybersecurity while also acting as a formidable weapon for cybercriminals.

Social Sciences Principles

As social sciences and technology intersect, the article describes how AI influences social norms, laws, and ethical principles. It shows the need to look into human actions in the cyber-space, highlighting the role of social sciences in this endeavor – the interpretation of AI-powered cyber crimes results. It creates the more broad question of whether technological advances threaten or benefit communities.

Research Questions or Hypotheses

At the article's core, Parti et al. (2023) studies how AI technologies augment the sophistication and reach of cybercrimes. It pertains to AI mechanisms helping automate and optimize phishing, malware dispersal and other cybercriminal strategies. It contends that AI integration into cybercrime develops unusual problems for cybersecurity defenses.

Research Methods

Parti et al. (2023) holistically see cybercrime using a thematic analysis that combines interviews, case studies, and a literature review under the qualitative research paradigm. Adopting this methodological approach allows for a deep inquiry into using AI for perverse purposes, producing illuminating representations of the dynamic cybersecurity atmosphere.

Data and Analysis

Parti et al. (2023) employed careful analysis to uncover AI misuse in cybercrime, such as deep fake generation and automation of social engineering schemes. The claim points out the difficulty of combating AI-driven cyber threats as it underlines the rate of modern criminals' transformations to use AI for criminal goals.

Concepts from PowerPoint Presentations

The article's discourse aligns with educational material on AI ethics and cybersecurity, wherein AI demonstrates theoretical aspects with practical contexts related to cybercrime. These theories materialize the doubts about the dilemmas posed by AI, social engineering psychology and imperative security measures.

Relevance to Marginalized Groups

Parti et al. (2023) point to the fact that AI-enabled cybercrime affects individuals differently, depending on the social location; it is observed that marginalized groups have greater risks. It demands a holistic cybersecurity attack that addresses the technology challenges but is

also responsive to the current socioeconomic inequalities, which may heighten the vulnerabilities of these groups.

Contributions to Society

Parti et al., (2023) significantly supplements the discussion on AI and cybercrime by shedding light on the issue's complexities and recommending a multi-stakeholder approach to cybersecurity. It argues for ethical AI development, rigorous policymaking, and intense public enlightenment as fundamental to safeguarding digital society from the criminal use of AI in cyberspace.

Conclusion

The articles studies will create contextual knowledge that serves as the building block of a better understanding of the pervasive between technology and its dark side. It demands coordinated action between technologists, policymakers, and the public to guarantee that the benefits of AI to society are optimized and the risks of malicious use are minimized.

Reference:

Parti, K., Dearden, T., & Choi, S. (2023). Understanding the use of artificial intelligence in Cybercrime. *International Journal of Cybersecurity Intelligence & Cybercrime*, *6*(2). https://doi.org/10.52306/2578-3289.1170